UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

GREG JOHNSON, individually and on behalf of all others similarly situated, Plaintiff, v. LEGACY PROFESSIONALS LLP, Defendant.	Case No.: JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Greg Johnson ("Plaintiff"), on behalf of himself and all others similarly situated, by and through his attorneys, brings this action against Legacy Professionals LLP ("Defendant") and alleges, upon his personal knowledge as to his own actions and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Financial services providers that collect and hold consumers' sensitive information, including their names, phone numbers, addresses, email addresses, dates of birth, financial account numbers, Social Security numbers and/or passport numbers ("Personally Identifiable Information" or "PII"), have a duty to clients to protect their valuable, sensitive information.

2. Defendant is a certified public accounting firm with offices in Illinois, Indiana, and Minnesota, that provides audits and accounting services, client accounting & advisory services, tax services, and payroll compliance audits, among other services.

3. As a corporation whose bread and butter requires the gathering of highly sensitive financial information, Defendant is well aware of the life-altering impact a data breach can wreak.

4. Despite Defendant's status as a sophisticated financial services provider, Defendant failed to properly protect clients by investing in adequate data security, thereby allowing hackers to exfiltrate the highly-sensitive PII entrusted to Defendant for accounting and other services. In approximately late April 2024, Defendant's failure to safeguard PII resulted in a data breach in which third party PII maintained by it was exfiltrated (the "Data Breach").

5. While the contents of the Data Breach have not yet been revealed, Defendant confirmed that the information lost in the Data Breach was posted on the dark web.[1] According to the Data Breach Notice, Defendant recognized suspicious activity in April of 2024, but failed to identify the files that had been exfiltrated until November 13, 2024, when Defendant learned of its data on the dark web.

6. Defendant did not communicate the Data Breach to clients and individuals until December 18, 2024. As a result, individuals like Plaintiff had no knowledge that their information was at risk for more than seven months, costing them valuable time during which they could have taken proactive measures to protect themselves and their data.

7. Notably, Defendant has not announced how many individuals have been impacted by the data breach and has not identified whose information was stolen in the breach.

8. Despite the highly sensitive nature of the personal information Defendant collected, and the prevalence of data breaches impacting financial services, Defendant inexplicably failed to implement and maintain reasonable and adequate security procedures and practices to safeguard the PII of Plaintiff and the Class. The Data Breach itself and information Defendant has disclosed about the breach to date, including the significant lapse between the Data Breach and Defendant's Notice, the need to remediate Defendant's cybersecurity, and the likely sensitive nature of the

[1] Ex. A, Legacy Professionals LLP Notice ("Notice")

impacted data, collectively demonstrate Defendant failed to implement reasonable measures to prevent the Data Breach and the exposure of highly sensitive information.

9. Defendant's failure to promptly notify Plaintiff and Class members that their PII was exfiltrated due to Defendant's security failures virtually ensured that the unauthorized third parties who exploited Defendant's security vulnerabilities could monetize, misuse, and/or disseminate that PII before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated even beyond the Data Breach itself.

10. Plaintiff and Class members had a reasonable expectation and understanding that Defendant would adopt adequate data security safeguards to protect their PII.

11. However, Defendant failed to: take sufficient and reasonable measures to safeguard its data security systems and protect highly sensitive data to prevent the Data Breach from occurring; to disclose to clients the material fact that it lacked appropriate data systems and security practices to secure PII; and to timely detect and provide adequate notice of the Data Breach to affected individuals. Because of Defendant's failures, Plaintiff and Class members suffered substantial harm and injury.

12. As a direct result of Defendant's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common law obligations, Plaintiff's and Class members' PII was accessed and acquired by unauthorized third parties for the purpose of misusing the data and causing further irreparable harm to the personal, financial, reputational, and future well-being of Defendant's clients.

13. Plaintiff and Class members face the real, immediate, and likely danger of identity

theft and misuse of their PII, especially because their PII was specifically targeted by malevolent actors. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe.

14. Plaintiff and Class members suffered injuries as a result of Defendant's conduct, including, but not limited to: diminished value of their PII; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; time needed to change usernames and passwords on their accounts; time needed to investigate, correct, and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach; charges and fees associated with fraudulent charges on their accounts; and the continued and increased risk of compromise to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect its PII. These risks will remain for the lifetimes of Plaintiff and the Class.

15. Plaintiff brings this action individually and on behalf of the Class, seeking relief including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorneys' fees and costs, and all other remedies this Court deems proper.

II. JURISDICTION AND VENUE

16. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of costs and interest. Moreover, because of the scope of Defendant's business, the Class likely includes

individuals from all over the United States, and Plaintiff reasonably believes there are more than 100 putative Class members.

17. Venue is proper in this judicial district under 28 U.S.C. § 1391 because Defendant is headquartered and transacts substantial business in this district, and because a substantial portion of the events giving rise to Plaintiff's claims occurred here.

18. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in Westchester, Illinois.

III. PARTIES

19. Plaintiff Greg Johnson is a resident of Cook County, Illinois and citizen of the United States. Plaintiff's PII was shared with Defendant as a financial services provider and Plaintiff reasonably believes that he has been impacted by the Data Breach.

20. Defendant Legacy Professionals LLP is a business entity with its principal place of business located in Westchester, Illinois.

IV. FACTUAL ALLEGATIONS

A. Defendant Collects Highly Sensitive Financial Information from Clients.

21. Defendant is a certified public accounting firm that provides audit, accounting, tax, and other related services to clients throughout the country. Defendant specializes in providing services to employee benefit plans, labor organizations, and commercial entities, among others.[2]

22. In order to provide accounting and other financial services, Defendant collects sensitive PII and financial information including, but not limited to, names, phone numbers, email

[2] https://www.legacycpas.com/practice-areas (last accessed December 19, 2024).

addresses, postal addresses, dates of birth, Social Security numbers, copies of government-issued identification documents such as driver's licenses, and financial account numbers.

23. As a result, Defendant hosts a large repository of sensitive personal information received from clients, including Plaintiff and the Class.

B. Defendant Failed to Adequately Protect Client Data, Resulting in the Breach.

24. Despite first detecting suspicious activity on Defendant's systems in late April 2024, Defendant remains unable to identify what files, or whose data, were implicated in the Data Breach.

25. Until November 13, 2024, Defendant believed that the suspicious activity in late April 2024 resulted "a small number of files" being accessed without authorization. Ex. A. Although Defendant claims to have received a "letter of containment" from a third-party cyber-specialist, a zip file taken from Defendant's systems was detected on the dark web on November 13, 2024.

26. On December 18, 2024, Defendant began notifying impacted clients of the Data Breach. Despite more than a month passing since Defendant discovered its data on the dark web, Defendant remains unable to identify the contents of the data or the scale of the Data Breach, including how many people have been impacted.

27. Defendant has not offered credit monitoring or identify protection services for individuals who have been impacted by the Data Breach.

28. Notably, Defendant's own Notice acknowledges that it failed to adequately protect PII, by detailing the "further enhancements" made to its security program since the Data Breach, including "[u]tilization of file level encryption on a network drive for sensitive data received from our clients", [a]n additional endpoint detection and threat hunting software Huntress to be active on all systems…", and "[a]round the clock SOC Monitoring of SentinelOne, Huntress, Microsoft

Office 365 ("O365") environment, and firewall by Arctic Wolf[.]" Ex. A.

29. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store PII, like Defendant, preceding the date of the Data Breach.

30. Data thieves regularly target institutions like Defendant due to the highly sensitive information in their custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

C. Defendant Failed to Take Adequate Actions Prior to and Following the Data Breach.

31. Defendant has an obligation to keep confidential and protect from unauthorized access and/or disclosure Plaintiff's and Class members' PII. Defendant's obligations are derived from: (1) government regulations and laws, including Federal Trade Commission ("FTC") rules; (2) industry standards; and (3) promises and representations regarding the handling of sensitive PII. Plaintiff and Class members provided—and Defendant obtained—their PII on the understanding that their PII would be protected and safeguarded from unauthorized access or disclosure.

32. Defendant claims that it "considers the security of [its] clients' data to be of utmost importance." Ex. A.

33. Defendant knew it was storing sensitive PII and that, as a result, its systems would be an attractive target for cybercriminals.

34. Cyber-attacks and ransomware attacks are frequently used to target companies or large entities due to the volume of sensitive data that they collect, maintain, and store.[3]

[3] Charles Griffiths, *The Latest 2024 Cyber Crime Statistics (updated July 2024)*, AAG (Jan. 7, 2024), available at https://aag-it.com/the-latest-cyber-crime-statistics/ (last accessed December 19, 2024).

35. Defendant could have prevented this Data Breach by properly encrypting or otherwise protecting its equipment and network files containing PII.

36. Despite widespread industry warnings, Defendant failed to implement and use reasonable security procedures and practices to protect Plaintiff's and similarly situated individuals' sensitive PII.

37. Defendant's failure to properly safeguard Plaintiff's and Class members' PII allowed unauthorized actors to access sensitive PII.

38. The Data Breach highlights the inadequacies inherent in Defendant's network monitoring procedures and security training protocols. If Defendant had properly monitored its cybersecurity systems and implemented a sufficient training protocol for its employees, it would have prevented the Data Breach, detected the Data Breach sooner, and/or have prevented the hackers from accessing PII.

39. Defendant's failure to timely notify Plaintiff and other victims of the Data Breach that their PII had been misappropriated precluded them from taking meaningful steps to safeguard their identities prior to the dissemination of their PII.

40. Defendant's delayed response only further exacerbated the consequences of the Data Breach brought on by its systemic IT failures.

41. Defendant's failures are three-fold. First, Defendant failed to timely secure its computer systems to protect clients' PII and sensitive financial information. Defendant allowed unauthorized actors to access and exfiltrate highly sensitive PII and other financial information from an unknown number of clients without detection.

42. Second, Defendant failed to timely notify affected individuals, including Plaintiff and Class members, that their highly sensitive PII had been accessed by unauthorized third parties.

Despite the breach stemming from activity in late April 2024, Defendant was unaware that its clients' data was on the dark web until November 13, 2024, and did not notify clients until December 18, 2024.

43. Third, Defendant made no effort to protect Plaintiff and the Class from the long-term consequences of Defendant's acts and omissions. Plaintiff's and Class members' PII, including their Social Security numbers, cannot be changed and will remain at risk long into the future. As a result, Plaintiff and the Class will remain at a heightened and unreasonable risk of identity theft for the remainder of their lives.

44. In short, Defendant's myriad failures, including the failure to timely detect the Data Breach and to timely notify Plaintiff and the Class that their PII had been accessed due to Defendant's security failures, allowed unauthorized individuals to access and misappropriate Plaintiff's and Class members' PII for an unknown amount of time before Defendant finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats.

45. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors and lead to considerable costs to consumers. According to Statista, during the first quarter of 2023 alone, more than six million data records were exposed worldwide through data breaches.[4] Indeed, cybercrime is slated to cost the world $10.5 trillion annually by 2025.[5]

---

[4] https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/ (last accessed December 19, 2024).

[5] Steve Morgan, *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*, Cybercrime Magazine (Nov. 13, 2020), available at https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (last accessed December 19, 2024).

46. Identity theft is the most common consequence of data breaches to consumers. A 2021 report concluded that more than half of all data breaches resulted in identity theft, including unauthorized access to a victim's financial accounts, opening new accounts in the victim's name, and using a victim's personal information for other fraudulent activities.[6]

47. As a result, PII is an invaluable commodity and the most frequent target of hackers.[7] Numerous sources cite dark web pricing for personal information, such as name, date of birth, and Social Security number, ranging from $40 to $200.[8]

48. Many tend to minimize the value of certain categories of PII, such as names, birthdates, addresses, and phone numbers. However, security experts agree that "[i]f you have someone's name and address, that is still valuable."[9] At the end of the day, "the more info you have, the more it is worth."[10]

49. Thefts of Social Security numbers present an even greater risk to consumers. Indeed, data breaches involving Social Security numbers are "incredibly alarming" because "[u]nlike a credit card number which can be changed, Social Security numbers . . . are hard to change, or cannot be changed."[11]

50. Even if victims whose Social Security numbers have been compromised are able to

---

[6] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), available at https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed December 19, 2024).

[7] *Id*.

[8] *Id*.

[9] Robert Lemos, *All about your 'fullz' and how hackers turn your personal data into dollars*, PCWorld (June 2, 2016), available at https://www.pcworld.com/article/414992/all-about-your-fullz-and-how-hackers-turn-your-personal-data-into-dollars.html (last accessed December 19, 2024).

[10] *Id.*

[11] Brian Naylor, *Victims Of Social Security Number Theft Find It's Hard To Bounce Back*, NPR (Feb. 9, 2015), available at https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed December 19, 2024).

change their Social Security numbers, the new number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[12]

51. According to the FTC, in 2021, around 20% of Americans were victims of identity theft, indicating that most Americans have either been a victim of identity theft or know someone who has.[13]

52. The fraudulent activity resulting from Defendant's Data Breach may not come to light for years, as there may be a time lag between when Plaintiff's and Class members' PII was stolen and when it is used, meaning there may be a delay between when the harm occurs versus when it is discovered.[14]

53. Beyond economic impacts, identity theft also leads to lasting emotional impacts; a majority of the victims of identity theft report increased stress levels, fatigue, and trust issues with family and friends and decreased energy.[15]

54. Despite the prevalence of public announcements of data breach and data security compromises and the risks posed by compromises of PII, Defendant failed to take proper action to protect the PII of Plaintiff and the Class from misappropriation. As a result, the injuries to Plaintiff and the Class were foreseeable and directly caused by Defendant's failure to implement or

---

[12] *Id*.
[13] *Consumer Sentinel Network Data Book 2021*, Federal Trade Commission (Feb. 2022), available at https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf (last accessed December 19, 2024).
[14] *Report to Congressional Requesters*, Government Accountability Office, at 29 (June 2007), available at https://www.gao.gov/assets/gao-07-737.pdf (last accessed December 19, 2024).
[15] *New Study by Identity Theft Resource Center Explores the Non-Economic Negative Impacts Caused by Identity Theft*, Identity Theft Resource Center (Oct. 18, 2018), available at https://www.idtheftcenter.org/post/new-study-by-identity-theft-resource-center-explores-the-non-economic-negative-impacts-caused-by-identity-theft/#:~:text=Due%20to%20their%20identity%20theft,at%20school%20(eight%20percent) (last accessed December 19, 2024).

maintain adequate data security measures for its clients.

E. Defendant's Conduct Violated the FTC Requirements for Safeguarding Client's PII.

55. The FTC rules, regulations, and guidelines obligate businesses to protect PII from unauthorized access or disclosure by unauthorized persons.

56. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.[16]

57. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[17]

58. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

59. The FTC further recommends that companies not maintain PII longer than is needed

[16] *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[17] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (October 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed December 19, 2024).

for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

60. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

61. At all relevant times, Defendant was fully aware of its obligation to protect its clients' PII because it is a sophisticated business entity that is in the business of maintaining and transmitting PII.

62. Defendant was also aware of the significant consequences of its failure to protect its clients' PII and knew that this data, if hacked, would injure individuals, including Plaintiff and Class members.

63. Defendant failed to comply with FTC rules, regulations, and guidelines and industry standards concerning the protection and security of PII. As evidenced by lapse in time between the Data Breach and the Notice, and nature of the Data Breach, among its many deficient practices, Defendant failed in, *inter alia*, the following respects:

a. Developing and employing adequate intrusion detection systems;

b. Engaging in regular reviews of audit logs and authentication records;

c. Developing and maintaining adequate data security systems to reduce the risk of

data breaches and cyberattacks;

d. Ensuring the confidentiality and integrity of clients' PII;

e. Protecting against any reasonably anticipated threats or hazards to the security or integrity of its clients' PII;

f. Implementing policies and procedures to prevent, detect, contain, and correct security violations;

g. Developing adequate policies and procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports;

h. Implementing technical policies, procedures, and safeguards for electronically stored information concerning PII that permit access for only those persons or programs that have specifically been granted access; and

i. Other similar measures to protect the security and confidentiality of its clients' PII.

64. Had Defendant implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced. Defendant could have prevented or detected the Data Breach prior to the hackers accessing Defendant's systems and extracting sensitive and personal information; the amount and/or types of PII accessed by the hackers could have been avoided or greatly reduced; and clients of Defendant would have been notified sooner, allowing them to promptly take protective and mitigating actions.

F. Defendant Failed to Follow Industry Standards for Safeguarding PII.

65. Despite its alleged commitments to protecting client data, Defendant does not follow industry standard practices in securing PII.

66. Several best practices have been identified that at a minimum should be implemented by businesses like Defendant's, including but not limited to, educating all employees;

strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

67. Best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

68. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented the following measures, as recommended by the United States Government:

a. Implement an awareness and training program.

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

d. Configure firewalls to block access to known malicious IP addresses.

e. Patch operating systems, software, and firmware on devices.

f. Set anti-virus and anti-malware programs to conduct regular scans automatically.

g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those

with a need for administrator accounts should only use them when necessary.

h. Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder. Consider disabling Remote Desktop protocol (RDP) if it is not being used.

k. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

l. Execute operating system environments or specific programs in a virtualized environment.

m. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[18]

69. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of Plaintiff's and the Class's PII.

70. Such measures are the existing and applicable industry standards. Defendant failed

[18] Department of Justice, How to Protect Your Networks from RANSOMWARE at 3, https://www.justice.gov/criminal/criminal-ccips/file/872771/dl (last accessed December 19, 2024).

to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

71. Given that Defendant was storing its clients' sensitive PII, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

V. CLASS ACTION ALLEGATIONS

72. Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Nationwide Class defined as:

> **All persons in the United States whose PII was accessed in the Data Breach announced by Defendant on December 18, 2024 (the "Nationwide Class").**

73. Excluded from the Class are Defendant, its executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change, or expand the Class definition after conducting discovery.

74. In addition, Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), an Illinois Subclass defined as:

> **All persons who are residents of the State of Illinois whose PII was accessed in the Data Breach announced by Defendant on December 18, 2024 (the "Illinois Subclass").**

75. Excluded from the Illinois Subclass are Defendant and its executives and officers, and the Judge(s) assigned to this case.

76. The Nationwide Class and the Illinois Subclass are collectively referred to herein as the "Class."

77. **Numerosity**: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. While the exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiff only through the discovery process, Plaintiff believes, and on that basis alleges, that at least thousands of individuals' PII was affected by the Data Breach. The members

of the Class will be identified through information and records in Defendant's possession, custody, and control.

78. **Existence and Predominance of Common Questions of Fact and Law**: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. Whether Defendant's data security and retention policies were unreasonable;

b. Whether Defendant failed to protect the confidential and highly sensitive information with which it was entrusted;

c. Whether Defendant owed a duty to Plaintiff and Class members to safeguard their PII;

d. Whether Defendant breached any legal duties in connection with the Data Breach;

e. Whether Defendant's conduct was intentional, reckless, willful, or negligent;

f. Whether an implied contract was created concerning the security of Plaintiff's and Class members' PII;

g. Whether Defendant breached that implied contract by failing to protect and keep secure Plaintiff's and Class members' PII and/or failing to timely and adequately notify Plaintiff and Class members of the Data Breach;

h. Whether Plaintiff and Class members suffered damages as a result of Defendant's conduct;

i. Whether Plaintiff and the Class are entitled to monetary damages, injunctive relief, and/or other remedies and, if so, the nature of any such relief.

79. **Typicality**: Plaintiff's claims are typical of the claims of the Class because Plaintiff

and all members of the Class were injured through Defendant's uniform misconduct. The actions and omissions that gave rise to Plaintiff's claims are the same that gave rise to the claims of every other Class member because Plaintiff and each Class member had their sensitive PII compromised in the Data Breach due to Defendant's misconduct, and there are no defenses that are unique to Plaintiff.

80. **Adequacy**: Plaintiff is an adequate representative because his interests do not conflict with the interests of the Class that he seeks to represent, he has retained counsel competent and highly experienced in complex class action litigation, and they intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

81. **Superiority**: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and members of the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to redress effectively the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, an economy of scale, and comprehensive supervision by a single court. Upon information and belief, members of the Class can be readily identified and notified based on Defendant's records.

82. Defendant has acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate final equitable relief with respect to the Class as a whole.

VI. CAUSES OF ACTION

COUNT I – NEGLIGENCE

(On Behalf of Plaintiff and the Class)

83. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

84. Defendant owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing the PII that Defendant collected.

85. Defendant owed a duty to Plaintiff and the Class to provide security, consistent with industry standards and FTC requirements, and to ensure that its cyber networks and systems, and the personnel responsible for them, adequately protected the PII that Defendant collected.

86. Defendant owed a duty to Plaintiff and the Class to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the victims of a data breach as soon as possible after it is discovered.

87. Defendant owed a duty of care to Plaintiff and the Class because they were the foreseeable and probable victims of any inadequate data security practices.

88. Defendant solicited, gathered, and stored the PII belonging to Plaintiff and the Class. Defendant knew or should have known it inadequately safeguarded this information.

89. Defendant knew that a breach of its systems would inflict significant monetary damages upon Plaintiff and Class members, and Defendant was therefore charged with a duty to adequately protect this critically sensitive information.

90. Defendant had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' highly sensitive PII was entrusted to Defendant on the understanding that adequate security precautions would be taken to protect the PII. Moreover, only Defendant had the

ability to protect its systems and the PII stored on them from attack.

91. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff, Class members, and their PII. Defendant breached its duties to Plaintiff and Class members by failing to: (1) secure its systems, servers, and networks, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement safeguards, policies, and procedures necessary to prevent this type of data breach.

92. Defendant has an affirmative duty to timely disclose the unauthorized access and theft of the PII belonging to Plaintiff and the Class so that Plaintiff and the Class can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

93. Defendant breached its duty to timely notify Plaintiff and Class members of the Data Breach by failing to provide direct notice to Plaintiff and the Class concerning the Data Breach until December 18, 2024.

94. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered a drastically increased risk of identity theft, relative to both the time period before the breach, as well as to the risk born by the general public, in addition to other damages, including but not limited to time and expenses incurred in mitigating the effects of the Data Breach.

95. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II – NEGLIGENCE *PER SE*

(On Behalf of Plaintiff and the Class)

96. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

97. Section 5 of FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting

commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendant, of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

98. Defendant violated the FTC rules and regulations obligating companies to use reasonable measures to protect PII by failing to comply with applicable industry standards, and by unduly delaying reasonable notice of the actual breach. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, the foreseeable consequences of the Data Breach, and the exposure of Plaintiff's and Class members' sensitive PII.

99. Defendant's violations of Section 5 of the FTC Act and other applicable standards constitute negligence *per se*.

100. Plaintiff and the Class are within the category of persons that Section 5 of the FTC Act was intended to protect.

101. The harm that occurred as a result of the Data Breach is the type of harm that Section 5 of the FTC Act was intended to guard against.

102. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

103. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendant's violations of Section 5 of the FTC Act.

104. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (1) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) improper disclosure of their PII; (3) breach of the confidentiality of their PII; (4) deprivation and diminution in the value of their PII, for which there is a well-established national and international market; (5) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (6) actual or attempted fraud.

COUNT III - BREACH OF FIDUCIARY DUTY

(On Behalf of Plaintiff and the Nationwide Class or in the alternative, the Illinois Subclass)

105. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

106. Plaintiff and class members allowed their PII to be shared with Defendant in confidence, believing that Defendant would protect that information. Plaintiff and class members would not have provided Defendant with this information had they known it would not be adequately protected.

107. Defendant's acceptance and storage of Plaintiff's and class members' PII created a fiduciary relationship between Defendant and Plaintiff and Class members. In light of this relationship, Defendant must act primarily for the benefit of its clients, which includes safeguarding and protecting Plaintiff's and Class members' PII.

108. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the system containing Plaintiff's and Class members' PII, failing to comply with the data

security guidelines set forth by the FTC, and otherwise failing to safeguard Plaintiff's and Class members' PII that it collected.

109. Plaintiff and class members relied on Defendant to exercise its discretion in implementing proper data security and Defendant was in an exclusive position to guard against the foreseeable threat of a data breach. Plaintiff and class members had no way to influence or verify the integrity of Defendant's data security practices.

110. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (1) substantially increased risks of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) actual identity theft; (3) improper disclosure of their PII; (4) breach of the confidentiality of their PII; (5) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (6) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

111. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

112. Plaintiff and Class members are entitled to damages incurred as a result of the Data Breach.

113. Plaintiff and Class members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to Class members.

COUNT IV – BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff and the Nationwide Class)

114. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

115. When Plaintiff and Class members allowed their PII to be shared with Defendant, they entered into implied contracts with Defendant, under which Defendant agreed to adopt reasonable safeguards complying with relevant laws, regulations, and industry practices, including the FTC Act, to protect their PII, and to timely notify them in the event of a data breach.

116. Defendant solicited and invited Plaintiff and Class members to provide their PII as a condition of Defendant's provision of services. Plaintiff and Class members accepted Defendant's offers and provided their PII to Defendant.

117. When entering implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant would implement reasonable data security measures and that Defendant's data security practices complied with relevant laws, regulations, and industry standards. Defendant knew or should have known that Plaintiff and Class members held this belief and expectation.

118. Implicit in the agreement between Plaintiff and Class members and Defendant was Defendant's obligation to: (1) adequately safeguard Plaintiff's and Class members' PII; (2) prevent unauthorized access and/or disclosure of Plaintiff's and Class members' PII; (3) provide Plaintiff and Class members with prompt and sufficient notice of any and all unauthorized access and/or disclosure of their PII; and (4) retain Plaintiff's and Class members' PII under conditions that kept such information secure and confidential.

119. Defendant's conduct in requiring clients to provide PII as a prerequisite for accounting or financial services illustrates Defendant's intent to be bound by an implied promise to adopt reasonable data security measures.

120. Plaintiff and Class members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

121. Plaintiff and Class members fully and adequately performed their obligations under the implied contracts with Defendant. They provided consideration and their PII to Defendant in exchange for accounting or other financial services and accepted Defendant's implied promise to adopt reasonable data security measures.

122. Defendant breached its implied contracts with Plaintiff and Class members by failing to safeguard their PII and by failing to provide them with timely and accurate notice of the Data Breach.

123. The losses and damages Plaintiff and Class members sustained, include, but are not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection

services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and

j. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

124. The damages sustained by Plaintiff and Class Members were the direct and proximate result of Defendant's material breaches of its agreement(s).

COUNT V – UNJUST ENRICHMENT

(On Behalf of Plaintiff and the Class)

125. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

126. Plaintiff and Class members conferred benefits upon Defendant by permitting their PII to be shared with Defendant so that Defendant could render services for payment. In exchange for the payments provided to Defendant, Defendant should have provided accounting or other services accompanied by Defendant's adequate safeguarding of the PII of Plaintiffs and Class members.

127. Defendant knew that a benefit was conferred on it and accepted, has accepted, or retained that benefit. Defendant profited from the payments for its services and used Plaintiff's and Class members' PII for business or associated purposes.

128. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead utilized cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over adequate security.

129. Under principles of equity and good conscience, Defendant should not be permitted to retain the full monetary benefit of its transactions. Defendant failed to adequately secure PII and, therefore, did not provide the full services for which it received payment. Plaintiff and Class members now must monitor their personal, immutable PII for the rest of their lives.

130. If Plaintiff and Class members had known that Defendant employed inadequate data security safeguards, they would not have agreed to providing Defendant with PII.

131. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered the various types of damages alleged herein.

132. Plaintiff and Class members have no adequate remedy at law. Defendant continues to retain Plaintiff's and Class members' PII, therefore exposing the PII to a risk of future data breaches in Defendant's possession.

133. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court enter a judgment on their behalf and against Defendant, and further grant the following relief:

A. Certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Designate Plaintiff as a representative of the proposed Nationwide Class and Illinois Subclass and Plaintiff's counsel as Class counsel;

C. Grant Plaintiff the declaratory relief sought herein;

D. Grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

E. Award Plaintiff and the Class compensatory, consequential, and general damages in an amount to be determined at trial, and any other relief to which they are entitled under the law;

F. Award Plaintiff and the Class statutory damages, and punitive or exemplary damages, to the extent permitted by law;

G. Award prejudgment interest, costs, and attorneys' fees;

H. Award all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

I. Award Plaintiff and the Class such other and further relief as the Court deems just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff, individually and on behalf of the proposed Class, respectfully requests a trial by jury as to all matters so triable.

DATED: December 20, 2024

Respectfully Submitted,

/s/ Elizabeth A. Fegan

Elizabeth A. Fegan
Megan E. Shannon
FEGAN SCOTT LLC
150 S. Wacker Drive, 24th Floor
Chicago, IL 60606
Telephone: (312) 741-1019
Facsimile: (312) 264-0100
beth@feganscott.com
megan@feganscott.com

Vincent D. Pinelli
BURKE BURNS & PINELLI, LTD.
Three First National Plaza —70 W. Madison St., Suite 4300
Chicago, IL 60602
Telephone: 312.541.8600
Facsimile: 312.541.8603
vpinelli@bbp-chicago.com

Attorneys for Plaintiff and the Proposed Class